Annexe 1 quater

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 172 239**
B1

(12) # EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: **03.05.89**

(51) Int. Cl.⁴: **G 06 F 1/00**

(21) Application number: **85901253.6**

(22) Date of filing: **21.02.85**

(86) International application number:
PCT/US85/00275

(87) International publication number:
WO 85/03785 29.08.85 Gazette 85/19

(54) **SOLID STATE KEY FOR CONTROLLING ACCESS TO COMPUTER SOFTWARE.**

(30) Priority: **22.02.84 US 582302**

(43) Date of publication of application:
26.02.86 Bulletin 86/09

(45) Publication of the grant of the patent:
03.05.89 Bulletin 89/18

(84) Designated Contracting States:
AT BE CH DE FR GB LI LU NL SE

(56) References cited:
GB-A-2 080 203
US-A-3 891 799
US-A-3 959 633
US-A-4 295 039
US-A-4 310 720
US-A-4 430 728
US-A-4 447 890
US-A-4 475 175
US-A-4 484 306
US-A-4 486 828
US-A-4 494 114
COMPUTER, vol. 17, no. 3, March 1984, page 99, Long Beach, Ca., US; "Security device eliminates passwords and encryption"

(73) Proprietor: **THUMBSCAN INC.**
Two Mid-America Plaza Suite 800
Oakbrook Terrace Illinois 60181 (US)

(72) Inventor: **CARGILE, William, P.**
2064 Touraine
Half Moon Bay, CA 94019 (US)

(74) Representative: **Calderbank, Thomas Roger et al**
MEWBURN ELLIS & CO. 2/3 Cursitor Street London EC4A 1BQ (GB)

EP 0 172 239 B1

Courier Press, Leamington Spa, England.

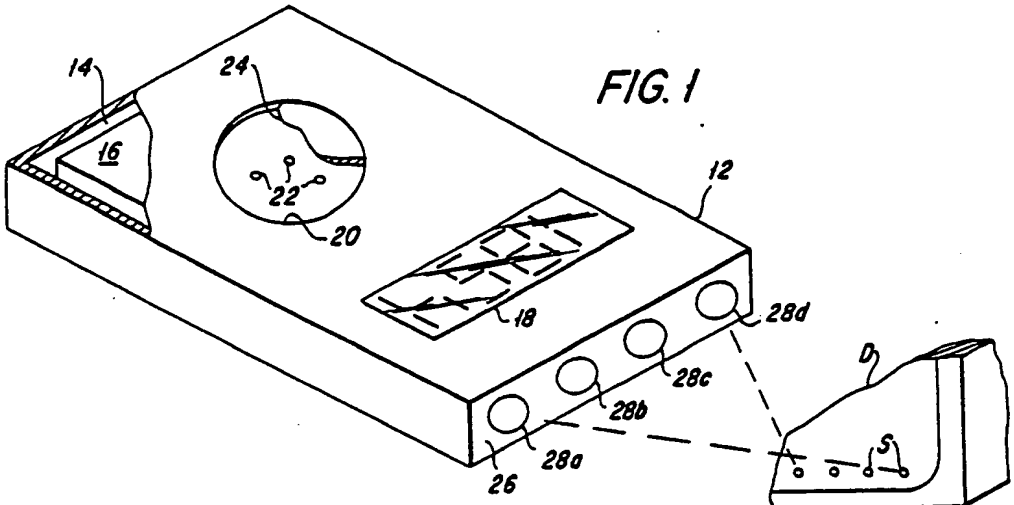
14
24
16
22
20
12
18
28d
28c
28b
28a
26
D
S

FIG. 1

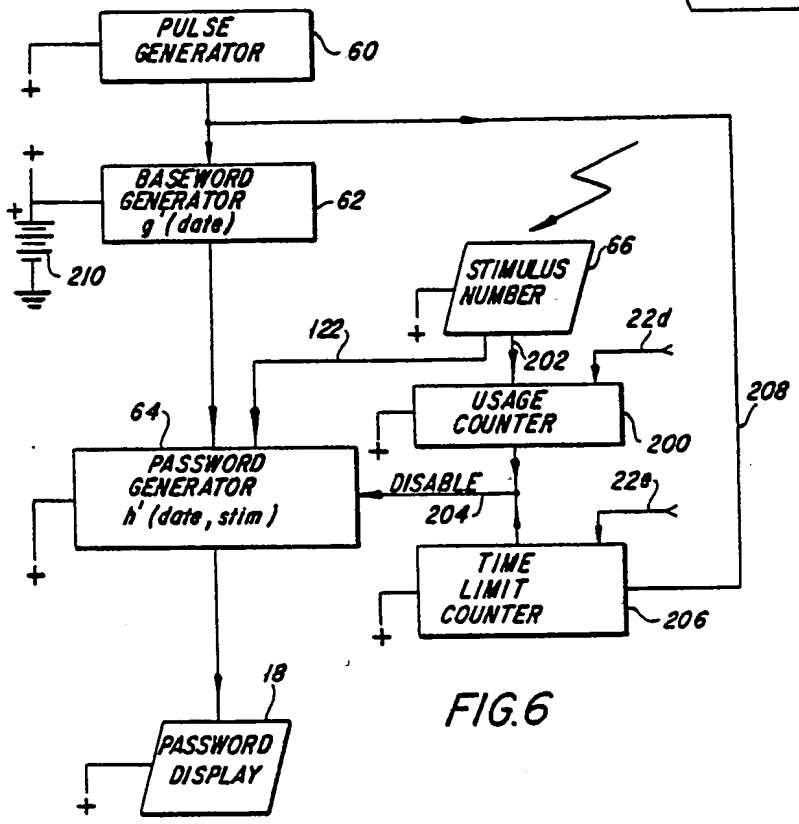
PULSE GENERATOR
60
BASEWORD GENERATOR g (date)
62
210
STIMULUS NUMBER
66
122
22d
202
USAGE COUNTER
200
208
64
PASSWORD GENERATOR h' (date, stim)
DISABLE
204
22e
TIME LIMIT COUNTER
206
18
PASSWORD DISPLAY

FIG. 6

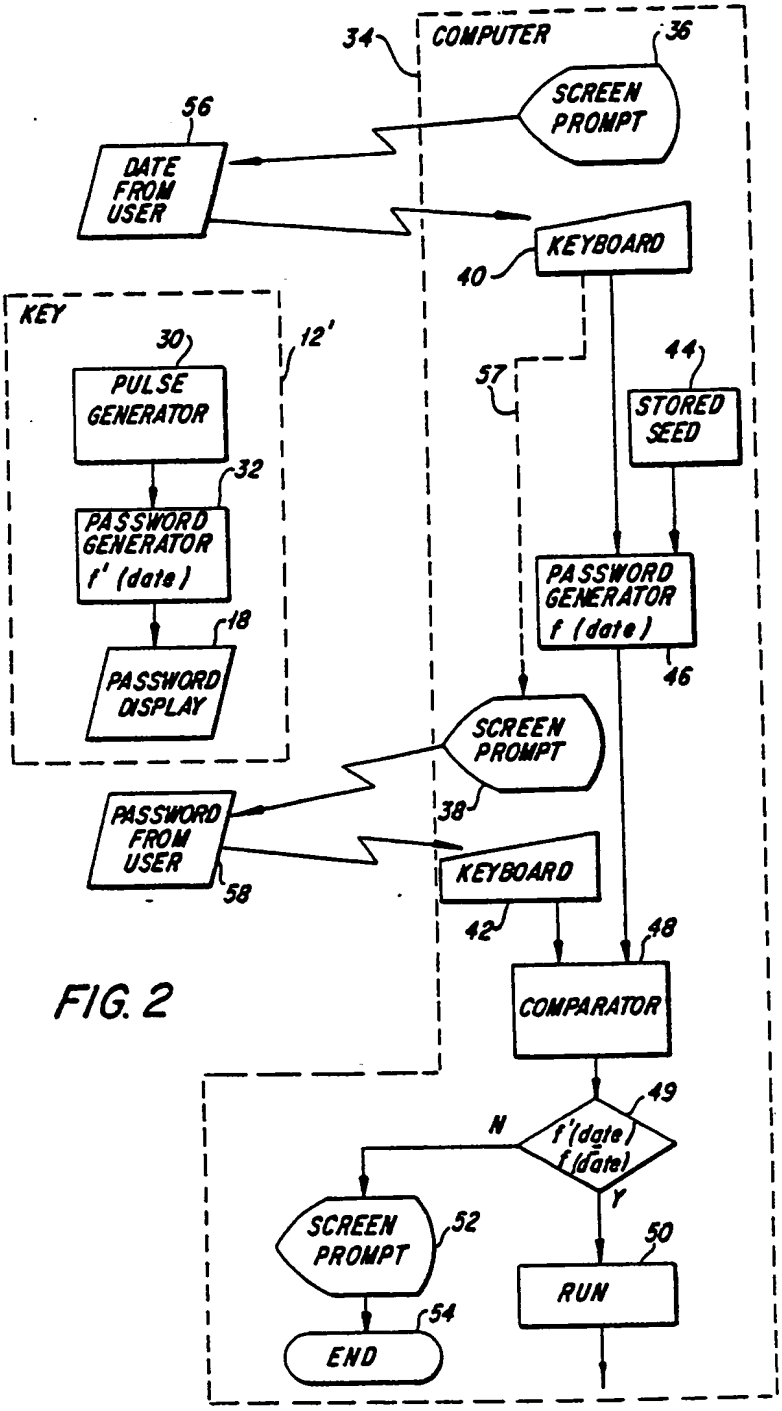
COMPUTER
34
36
SCREEN PROMPT
56
DATE FROM USER
KEYBOARD
40
KEY
12'
30
PULSE GENERATOR
32
PASSWORD GENERATOR f' (date)
18
PASSWORD DISPLAY
57
44
STORED SEED
PASSWORD GENERATOR f (date)
46
SCREEN PROMPT
38
PASSWORD FROM USER
58
KEYBOARD
42
48
COMPARATOR
49
N
f'(date) = f(date)
Y
SCREEN PROMPT
52
50
RUN
54
END

FIG. 2

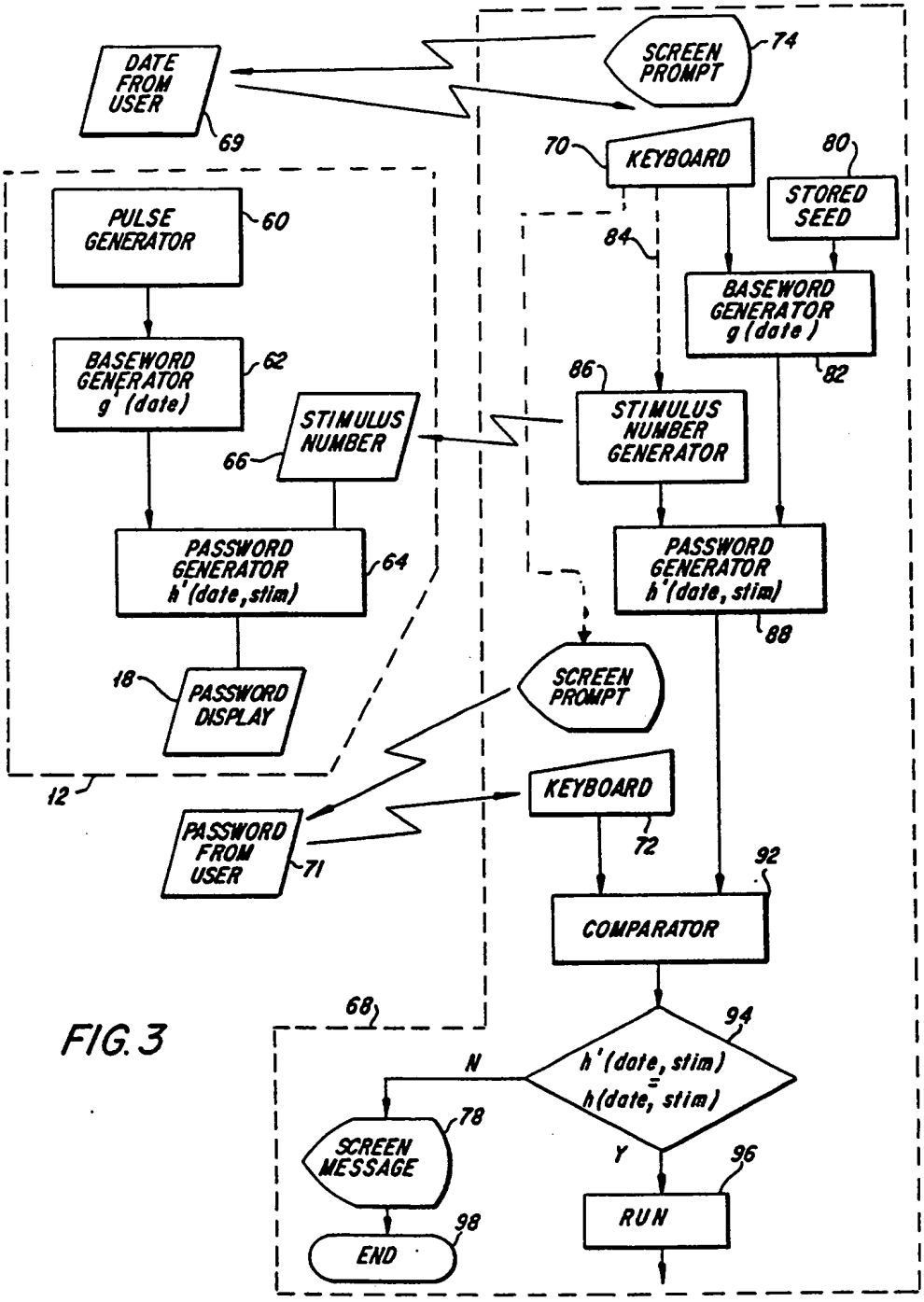
DATE FROM USER
69
SCREEN PROMPT
74
70
KEYBOARD
80
STORED SEED
PULSE GENERATOR
60
84
BASEWORD GENERATOR g(date)
82
BASEWORD GENERATOR g'(date)
62
86
STIMULUS NUMBER
66
STIMULUS NUMBER GENERATOR
PASSWORD GENERATOR h'(date,stim)
64
PASSWORD GENERATOR h'(date, stim)
88
18
PASSWORD DISPLAY
SCREEN PROMPT
12
KEYBOARD
72
PASSWORD FROM USER
71
92
COMPARATOR
68
94
N
h'(date, stim) = h(date, stim)
78
SCREEN MESSAGE
Y
96
RUN
98
END

FIG. 3

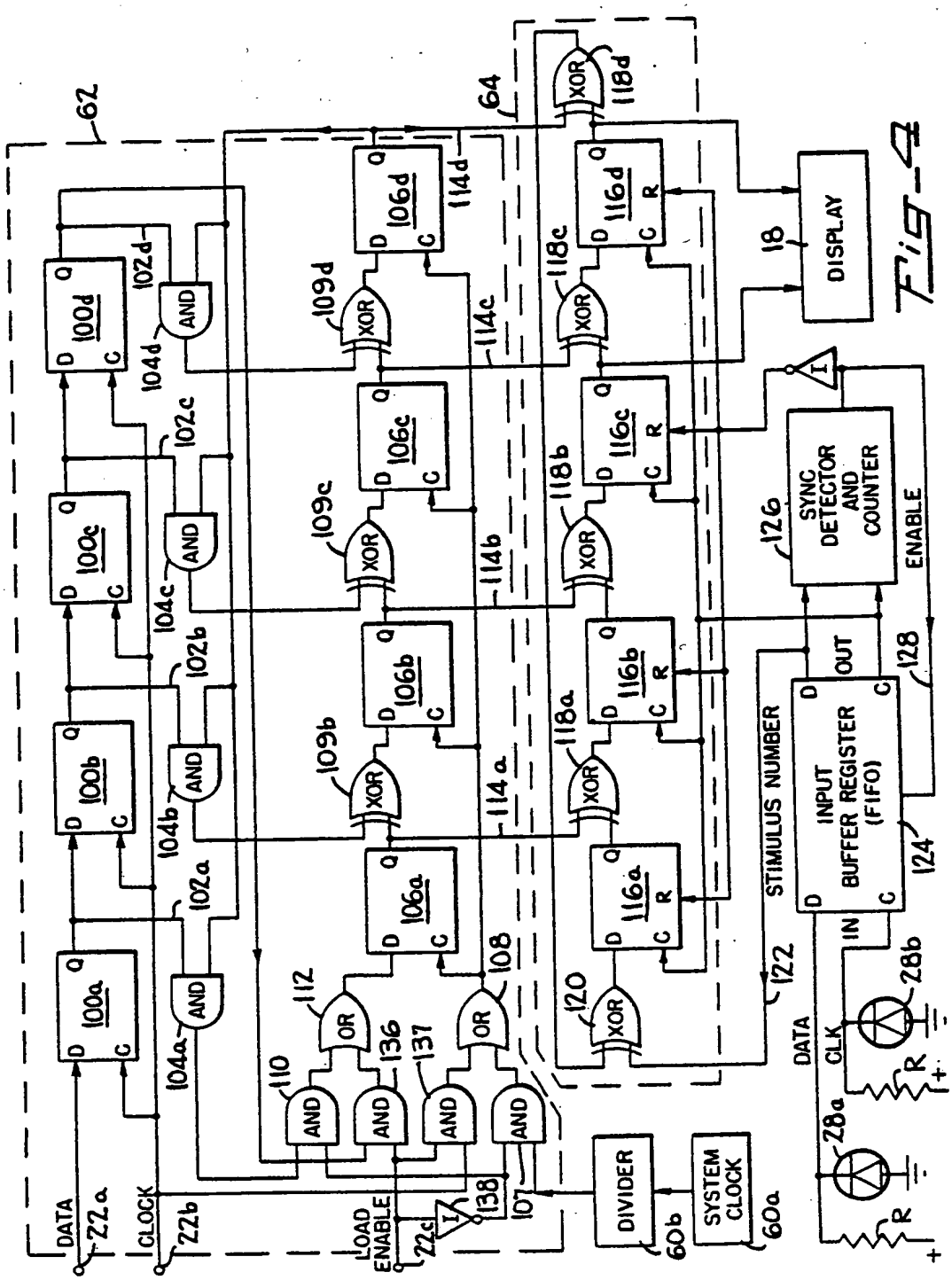
62
64
DATA
22a
CLOCK
22b
LOAD ENABLE
22c
100a
100b
100c
100d
102a
102b
102c
102d
104a
104b
104c
104d
106a
106b
106c
106d
108
109b
109c
109d
110
112
114a
114b
114c
114d
116a
116b
116c
116d
118a
118b
118c
118d
120
122
124
126
128
136
137
138
107
AND
OR
XOR
DIVIDER
60b
SYSTEM CLOCK
60a
DISPLAY
18
SYNC DETECTOR AND COUNTER
ENABLE
STIMULUS NUMBER
INPUT BUFFER REGISTER (FIFO)
OUT
IN
DATA
CLK
28a
28b
R
+

Fig. 4

FLIP-FLOP ID	100a	100b	100c	100d	140
OUTPUT STATE(Q)	0	1	0	1	
FLIP-FLOP ID	106a	106b	106c	106d	142
OUTPUT STATE(Q) (DAY 0)	1	1	0	0	
FLIP-FLOP ID	116a	116b	116c	116d	144
INITIAL	0	0	0	0	
STIM NUM = 1 CLOCK 1	1	1	1	0	146
STIM NUM = 1 CLOCK 2	1	0	0	1	
STIM NUM = 1 CLOCK 3	0	0	1	0	
STIM NUM = 0 CLOCK 4	0	1	[1] 181	[1]	
INITIAL	0	0	0	0	
STIM NUM = 0 CLOCK 1	0	1	1	0	148
STIM NUM = 1 CLOCK 2	1	1	0	1	
STIM NUM = 0 CLOCK 3	1	0	0	0	
STIM NUM = 0 CLOCK 4	0	0	[1] 182	[0]	
FLIP-FLOP ID	106a	106b	106c	106d	150
OUTPUT STATE(Q) (DAY 1)	0	1	1	0	
FLIP-FLOP ID	116a	116b	116c	116d	
INITIAL	0	0	0	0	
STIM NUM = 1 CLOCK 1	1	0	1	1	152
STIM NUM = 1 CLOCK 2	0	1	1	0	
STIM NUM = 1 CLOCK 3	1	0	0	0	
STIM NUM = 1 CLOCK 4	1	1	[1] 183	[1]	

FIG. 5

Description

This invention relates to apparatus for affording access to computer software only by authorized persons, and more particularly to apparatus physically independent of the computer equipment but capable of executing an algorithm that can also be executed by the computer equipment to afford access.

Computer software, whether in the form of an operating system program or an application program, is typically stored in media that afford convenient access to a user. Exemplifying such media are main computer memory as well as peripherals such as magnetic disks, magnetic diskettes or magnetic tape. Software on such media requires substantial time and money to develop and it is desired in most cases to limit access to the software to only certain persons.

Numerous techniques for limiting access to computer software are practiced. In multiuser systems it is typical for each user to have an identification code and/or a password which the user must enter before gaining access to the system. Security of the software can be compromised when an authorized user reveals his or her identification code and/or password to unauthorized persons or the access code is discovered by a persistent hacker.

Another technique employed, particularly with respect to application software that is provided on magnetic diskettes, is to encode on the diskette a protective routine that causes the operating system to disable any copying facilities within it. This technique has had only moderate success in preventing unauthorized use or unauthorized copying because programs for disabling such protective routines are widely available.

Although the above described techniques and the copyright laws have impeded unauthorized use and/or copying of computer software, the creators of software continue to experience losses as a result of the activities of unprincipled copiers. This had impeded the creation of software and the allocation of resources necessary to the creation of software.

US—A—4295039 discloses a system for affording access by a user to a software program residing in a computer. The system has an access key which generates a password. The computer contains an access key verification means which verifies the password from the access key, and on that verification allows access to and use of the software program. The access key is transportable independently of the computer. This document therefore corresponds to the pre-characterising part of claim 1.

US—A—4310720 discloses another system for affording access to a computer having an access key which generates a password from an initial grouping of said numbers, the password then being verified by suitable verification means within the computer. Again the access key is capable of being transported independently of the computer.

The present invention seeks to improve such systems and, according to a first aspect of the invention, the access key includes:

(a) pulse generating means for generating a signal that is dependent on the elapse of time;

(b) password generating means coupled to said pulse generating means for generating a password from the signal from said pulse generating means;

(c) displaying means communicating with the password generating means for displaying at least part of said password.

Furthermore, the access key verification means includes:

(a) means for receiving at least initially a time input;

(b) means for recieving the password as generated by the access key and input by the user;

(c) means for processing the time input for producing an internal password;

(d) means for determining if the internal password bears a prescribed relationship to the password generated by said access key;

(e) means for affording access to the software program if the prescribed relationship exists.

In addition, according to another aspect of the invention there is provided an access key for affording access by a user to a software program, said access key comprising:

(a) pulse generating means for generating a series of pulses that are dependent on the elapse of time;

(b) password generating means coupled to said pulse generating means for generating a password for one or more pulses from said pulse generating means;

(c) displaying means communicating with the password generating means for displaying at least part of said password;

(d) at least one sensor accessible from the exterior of said access key so that a coded stimulus is receivable by said access key;

(e) means coupled to said sensor for decoding the stimulus number;

(f) said password generating means for combining the stimulus number with the one or more pulses from the pulse generator to produce the password.

In order for the software in the computer to be able to produce an internal password for comparison with the user input password, the user is first prompted by the computer to enter the current date. The computer manipulates the current date by an algorithm corresponding to that in the key to produce the internal password.

An important aspect of the invention is that the shift register within the key is pre-loaded at manufacturing time with a unique number so that the likelihood of two keys being the same unique numbers is insignificant. For example, if the size of the shift register in the key is 32 bits, a size easily achievable under the present state of the art, there are almost five billion bit combinations that can be produced. Because the key is active,

i.e., because a continuous supply of power is necessary to maintain the register state, disassembly of the key for the purposes of ascertaining the function is virtually impossible because in disassembly it is highly likely that power to the shift register would be interrupted.

An enhanced version of a software access key embodying the invention, which is even more difficult for unauthorized persons to decode, involves an extra step to produce a password for input by the user. As in the version to which reference has been previously made, the key contains a shift register whose state changes with elapsed real time. The computer with which the key is adapted to cooperate is coded to generate a stimulus number which can be randomly generated and which is saved within the host computer. The stimulus number is transmitted to the key without direct connection, one technique for so transmitting the stimulus number involves excitation of one or more predetermined sites on the video display of the host computer and providing in the key two or more photo-sensors which respond to the pattern of excitation of the sites. The key includes circuitry for decoding the pattern of excitation at the display sites and generating a password from a combination of the decoded signal and the output of the above mentioned register that changes with real time. In practicing the invention employing the enhanced version, the association between the password displayed to the user and the current date as manifested by the output of the timer within the key is even more tenuous and therefore more difficult, if not impossible, to display by reverse engineering.

An object of the invention is to provide a hardware device that must be employed to gain access to computer software. This object is achieved by producing and displaying a password which must be input by the user and by so arranging the circuitry in the key that it produces, each time the device is used, a different password in accordance with an algorithm that is virtually impossible to predict.

Another object of the invention is to provide a device of the type described above that is inexpensive, portable and longlasting. The advent of large scale integrated circuit technology, such as manifested in existent wristwatches and the like, permits a key in accordance with the invention to be produced at a moderate cost, particularly when compared to the cost of many software programs.

A feature and advantage of the invention is that it employs digital techniques which afford exponential expansion of the number of possible combinations by merely extending by one or more bits the size of the numbers that the apparatus employs in producing a password.

The foregoing, together with other objects, features and advantages, will be more apparent after referring to the following specification and the accompanying drawings, in which:

Figure 1 is a perspective of a computer access key embodying the invention with portions being broken away to reveal internal details.

Figure 2 is a block diagram showing the interaction between a relatively uncomplex key in accordance with the invention and a computer containing code in accordance with the invention.

Figure 3 is a block diagram similar to Figure 2 but showing an enhanced key according to the invention.

Figure 4 is a block diagram of exemplary circuitry within the key of Figure 3.

Figure 5 is a table showing logical states at various points in the circuit of Figure 4 during a typical operating sequence.

Figure 6 is a block diagram of a key showing various enhancements in accordance with the invention.

Referring more particularly to the drawings, reference numeral 12 indicates a key embodying the present invention. The key includes a housing of plastic or like imperforate material which is hollow so as to define a central cavity 14. Within cavity 14 are elements, such as an integrated circuit device indicated fragmentarily at 16. Accessible from the exterior of the imperforate housing is a display 18 formed of conventional numeric or alphanumeric display elements, there being four numeric display elements in the embodiment shown in Figure 1. Such elements are typically liquid crystal display or LCD elements. In the specific example seen in Figure 1 display 18 displays the password or a displayed character representation "1854."

The top surface of key 12 is formed with a circular recess 20. The bottom surface of the recess contains one or more contact points 22, or openings in alignment with contact points within cavity 14, for establishing electrical contact with the circuitry 16 within the key. The contact points are employed when the key is set or initialized during manufacture to load a code or bit pattern that is unique to each user. After the key has been so set, a disk shaped cover 24 is installed in recess 20 to insulate contacts 22. Disk shaped cover 24 can be an adhesive backed label having an outer surface containing trademark or product identifying information.

Key 12 has a front face 26. Mounted within face 26 and accessible from the exterior of key are sensors 28a, 28b, 28c and 28d. In the specific embodiment shown in the drawings sensors 28a—28d are photoelectric diodes which respond to images formed on the video display screen D of the computer system containing software to which access is to be had. A fragment of video display screen D is shown at reduced scale in Figure 1. As will be described subsequently, predetermined sites S on the screen are excited in an appropriate time-space pattern to produce a signal that is received by key 12 by way of sensors 28a—28d. The sensors and the sites on the computer video display exemplify an information transmission link that uses radiant energy and not direct connection between the key and the computer. Other useful forms of radiant energy are sonic energy or radio frequency energy.

Referring to Figure 2, there is a key 12' which is

somewhat less complex than that shown in Figure 1 in that key 12' is not equipped with sensors 28a—28d. Key 12 includes a crystal controlled pulse generator 30 that produces a series of timing pulses that count real time. In one device designed in accordance with the invention, pulse generator 30 produces one pulse per day. The timing pulses supplied by pulse generator 30 are coupled to a password generator 32. The password generator produces a unique combination of binary digits depending on the number of date pulses that have been supplied to it by pulse generator 30 since initialization. Thus the binary bit pattern produced by password generator 32 is a function of the current date, referred to in this description and in Figure 2 as f'(date).

As will be described in more detail hereinafter in connection with the embodiment of Figures 3 and 4, password generator 32 can be embodied in a shift register into which pulses from pulse generator 30 are introduced serially and which produces a bit pattern representing f'(date) at parallel outputs. The specific number of bits produced by the password generator depends more on the number of keys that are to be distributed than circuit capabilities. Because the active components of key 12' are formed of large scale integrated circuits, a virtually unlimited number of bits can be provided in a very small volume.

At least some of the parallel outputs of password generator 32 are connected to a password display 18 which, in one device designed in accordance with the invention, is constituted by a plurality of LCDs. In order to limit the number of digits that a user must input to the computer containing the software to which access is desired, fewer bits are displayed by display 18 than are produced by password generator 32.

It will be seen then that key 12' produces on display 18 a number f'(date) that is a function of the date. In order to render the key immune to reverse engineering or decoding by a persistent hacker, it is preferred that the function f'(date) be such that the relation between the number of date pulses coupled to password generator 32 and the bit pattern output by the password generator not be an inverse relation. In order to facilitate understanding of password generation, the computer and the program resident in it will be described.

Reference numeral 34 indicates a computer containing a software program to which access is sought. The computer can be mainframe, mini or micro and includes a video display screen on which user prompts, indicated at 36 and 38, can be displayed. The computer also includes a keyboard to afford user input, indicated schematically at 40 and 42.

Computer 34 contains a stored seed number schematically represented at 44. The value of the stored seed is representative of the number or state to which password generator 32 in the key has been initialized. The value of the stored seed uniquely associates the key and the software program resident in computer 34. The computer also includes code for executing a password-generating algorithm, indicated diagrammatically at 46, so that the computer can produce, from the combination of the current date input by the user to keyboard 40 and stored seed 44, a password f(date) which corresponds to the password produced in key 12' and displayed on display 18. Also within computer 34 is comparison logic indicated at 48 for comparing the password generated by password generator 46 and the password input by the user to keyboard 42. Decision logic 49 determines subsequent action depending on whether correspondence between f(date) and f'(date) exists. Correspondence between the two passwords causes the protected software to run, indicated schematically at 50; inequality results in a screen prompt or message to the user, indicated at 52, and termination of the attempted access to the program, indicated at 54.

Equality between the functions f(date) and f'(date) is but one example of a predetermined or prescribed relationship between the functions. Another exemplary relationship involves using f(date) as an encryption key and f'(date) as a decryption key.

The operation of the system described to this point requires the user to activate computer 34 so that the video display requests the user via screen prompt 36 to input the current date to the computer. The user's compliance with the screen prompt is schematically indicated at 56, and the date is typed into the computer via keyboard 40. The date supplied to keyboard 40 is coupled to password generator 46 which, is alluded to previously, produces a password that is a function, f(date), of the current date. Such password is applied as one input to comparator 48. Another consequence of a date in proper form being applied to the keyboard is that the computer produces via a control path 57 a second screen prompt, indicated at 38, which instructs the user to input the user's password. The password is produced by key 12' and displayed on display 18. The user's input of the password gleaned from display 18 is indicated schematically at 58, the password being typed into the computer keyboard at 42. The password so typed in by the user is supplied as another input to comparator 48. The comparator 48 supplies a signal to decision logic 49, and if the password f(date) generated within the computer by password generator 46 corresponds to the password f'(date) input at keyboard 42, the software program is caused to run as at 50, that is, the user is afforded access to the software program. If the comparison fails, decision logic 49 causes creation of a screen prompt indicated at 52 informing the user that access to the computer software is denied.

Numerous characteristics of the present invention make it difficult, if not impossible, to decode by reverse engineering or other techniques. The number stored in password generator 32 is stored in a dynamic shift register so that attempted disassembly of the key, which would almost inevitably entail interruption of battery power to

the shift register, will destroy the number or state within password generator 32. Because of the relation, f'(date), between the date and the password displayed by display 18 is not an inverse function, a person obtaining possession of key 12' cannot derive the function f'(date) from observing a sequence of passwords displayed on display 18. Within computer 34, even the most readily copyable medium, a diskette, cannot be conveniently employed to decode the seed or the function f'(date). Such is the case because the seed can be embedded in data or code within the diskette at a different location from the logic that is called to effect password generation in response to keyboard input of the current date. Thus a significant degree of security is afforded.

The embodiment shown in Figures 3 and 4 exploits sensors 28a—28d to afford a key having even greater immunity to unauthorized decoding or reverse engineering. Referring to Figure 3, key 12 includes a pulse generator 60 which is substantially identical to pulse generator 30 described above in connection with Figure 2 in that pulse generator 60 produces pulses at a rate depending on the elapse of real time, for example one pulse per day. The output of pulse generator 60 is coupled to a baseword generator 62. Baseword generator 62 is similar in many respects to password generator 32 described in connection with Figure 2. Baseword generator 62 is typically embodied in a shift register having a serial input and plural parallel outputs. Pulses from pulse generator 60 are coupled to the serial input and the combination of the bit states at parallel output forms a number that is a function, g'(date), of elapsed time, i.e., the total number of pulses that have been produced by pulse generator 60 since initialization. Baseword generator 62 is initialized at the time of manufacture with a unique bit pattern; because the baseword generator is typically embodied in a silicon chip, the possible number of unique bit patterns is virtually unlimited. The parallel outputs of baseword generator are coupled as one input to a password generator 64. The other input of password generator 64 is supplied from a stimulus number input 66 via sensors 28a—28d. Password generator 64 produces an output that is a function of both the baseword, in turn a function of the date, and the stimulus number, such function being referred to herein as h'(date, stim), "stim". being an abbreviation for stimulus number. The output of password generator 64 is a plurality of bit states in parallel and selected ones of the bits are made accessible to the user via display 18 to which the password generator output is coupled.

Key 12 is adapted for use with a computer system 68 which is similar to that described above in connection with Figure 2. Computer 68 also contains software capable of executing an algorithm somewhat different from that described previously. Computer 68 has a keyboard; the user of the key supplies to the computer from the keyboard the current date as indicated at 69 and 70 and the password as indicated at 71 and 72. Computer 68 also has a display screen D (Figure 1), such as a video display, for prompting the user, screen prompts being illustrated in Figure 3 at 74, 76 and 78. The computer or the program loaded thereinto has a stored seed, indicated at 80, which is uniquely associated with the state at which baseword generator is initialized at manufacturing time so that key 12 and the medium in which the stored seed exits are uniquely associated throughout the useful life of the apparatus.

Computer 68 also includes software code so that the computer can function as a baseword generator 82 and produce a baseword that is a function, g(date) of both the date input by the user to keyboard 70 and the stored seed 80. The output of baseword generator 62 in key 12 and the output of baseword generator 82 in computer 68 bear a prescribed relationship to one another, typically equality. There is a control path 84 from keyboard 70 to a stimulus number generator 86 so that when user inputs a date to keyboard 70, stimulus number generator 86 is activated to produce an output which can be a random or arbitrarily varying number. The stimulus number produced by stimulus number generator 86 is utilized in two ways. First the stimulus number is saved as one input to a password generator 88. Second the stimulus number is processed by the computer to produce a time-space pattern on screen sites S for transmission of information that can be sensed by sensor 28a—28d. The user can place key 12 adjacent the computer display such that sensor 28a—28d are excited by radiation from the screen sites so that a signal representative of the output of stimulus number generator 86 is applied to password generator 64 in the key.

Password generator 88 produces a function h(date, stim) which bears a prescribed relationship to the password produced by password generator 64, equality being the typical relationship. The password displayed on display 18 is input to computer 68, element 71 representing the user's input and element 72 representing reception at the computer keyboard of the password. The password input by the user and the password generated by password generator 88 are compared by the computer which is coded so as to form a comparator 92. There is decision logic 94 within computer 68, and if correspondence between the computer generated password and the user input password is detected, the software program to which access is to be controlled is run as indicated at 96. If, to the contrary, lack of correspondence between the two passwords is detected, a screen message is produced, as indicated at 78, and access to the software program is denied, indicated at 98.

In further explanation of the construction of key 12, reference is made to Figure 4. In Figure 4 discrete logical elements are shown solely for the purpose of illustration, because the preferred embodiment of the invention incorporates the circuit functions within one or more silicon chips. In Figure 4, at the upper portion thereof, are four

data type flip-flops 100a, 100b, 100c and 100d. The flip-flops form a shift register having four outputs identified at 102a, 102b, 102c and 102d. The state of the flip-flops 100a—100d, and therefore the bit pattern appearing at outputs 102a—102d, remains constant throughout the life of the key, and after initialization uniquely identifies a single user. Although four flip-flops provide only sixteen combinations of unique numbers or functions it is reiterated that Figure 4 is for the purpose of illustration and is not for the purpose of limitation.

As will appear, the state of flip-flops 100a—100d defines the function g' referred to previously in connection with element 62 of Figure 3 to which the timing pulses from pulse generator 60 are subjected to produce the baseword g'(date). Parallel outputs 102a—102d are connected as inputs to respective AND gates 104a, 104b, 104c and 104d.

The outputs of AND gates 104a—104d are gated to the input of respective data type flip-flops 106a, 106b, 106c and 106d. Flip-flops 106a—106d have clock inputs to which the output of pulse generator 60 is coupled; in Figure 4 pulse generator 60 is shown as a crystal controlled oscillator that constitutes a system clock 60a which produces system clock pulses at a relatively high rate and a divider circuit 60b which divides the relatively high frequency pulses produced by the system clock so that the output of the divide circuit provides a pulse at a repetition rate of one per day. Divide circuit 60b is coupled to the clock inputs of flip-flops 106a—106d through an AND age 107 and an OR gate 108. Each AND gate 104a—104d includes a second input to which is coupled the Q output of flip-flop 106d. The outputs of AND gates 104a—104d thus depend on the state of flip-flop 106d and the states of respective flip-flops 100a—100d. The D inputs of flip-flops 106b—106d are supplied through respective XOR gates 109b, 109c and 109d which have one input coupled to respective AND gates 104b—104d and another input coupled to the output of the preceding flip-flop, namely: 106a—106c, respectively. The input to flip-flop 106a is supplied by AND gate 104a through AND gate 110 and an OR gate 112. After initialization during manufacture, AND gate 110 is continuously enabled so that during the life of key 12 operation occurs as though AND gate 104a were directly connected to the D input of flip-flop 106a.

Flip-flops 100a—100d together with AND gates 104a—104d and XOR gates 109b—109d cooperate to produce the function g'(date). Thus flip-flops 106a—106d have respective outputs 114a—114d the bit pattern of which corresponds to the baseword, g'(date). As such the bit pattern appearing on outputs 114a—114d changes once each day to a number that is the function of the number of pulses supplied by divider circuit 60b and the state stored in flip-flops 100a—100d

The baseword is coupled to a pass word generator 64 which includes data type flip flops 116a, 116b, 116c and 116d. There are four XOR gates 118a, 118b, 118c and 118d, each of which has one input driven by the respective Q outputs of flip-flops 106a—106d and the other input driven by respective flip-flops 116a—116d. The output of XOR gate 118a is coupled to the D input of flip-flop 116b, the output of XOR gate 118b is coupled to the D input of flip-flop 116c, the output of XOR gate 118c is coupled to the D input of flip-flop 116d and the output of XOR gate 118d is coupled to the D input of flip-flop 116a through an XOR gate 120. To the other input of XOR gate 120 via a circuit path 122 is coupled the stimulus number received by sensors 28a—28d and indicated in Figure 3 at 66.

Two sensors, such as sensor 28a and 28d are shown in Figure 4. The other two sensors, 28b and 28c, are omitted for simplicity because their outputs are handled in substantially the same manner as is the output of sensor 28a. The sensors are biased by pull up resistors R which are connected to the positive terminal of the battery power supply within key 12. The outputs of the sensors constitute inputs to an input buffer register 124. Buffer register 124 is a FIFO register. The register has a plurality of data inputs one of which is shown coupled to the output of sensor 28a and a clock input shown coupled to the output of sensor 28b. The buffer register has a Q output, on which data appears, and a clock output. The data and clock outputs of input register 124 are coupled to a sync detector and counter 126. Sync detector 126 is a well known circuit which detects a prescribed pattern and number of signals supplied to it from buffer register 124 to ascertain when a data signal, in contrast to noise or the like, has been applied to the sensors. When ascertainment of data signals is made, sync detector supplies via a circuit path 128 an enable signal to input register 124. In response to receipt of an enable signal, the input register supplies data to XOR gate 120 via circuit path 122. Sync detector and counter 126 includes a counter which counts a prescribed number of pulses (four in the exemplary circuit of Figure 4) and applies an enable signal on circuit path 128 for a period corresponding to the duration of the prescribed number of pulses. There is an inverter 129 coupled from circuit path 128 to the reset inputs of flip-flops 116a—116d. When there is no enable signal on circuit path 128, the action of inverter is such as to reset flip-flops 116a—116d so that the state of their respective outputs is 0. When a stimulus number of proper format is received, the enable signal is asserted and the reset signal to flip-flops 116a—116d is discontinued so that the stimulus number can be loaded into the shift register constituted by the latter flip-flops.

The bits appearing at the outputs of flip-flops 116c and 116d are displayed to the user on display 18. Because Figure 4 has been reduced and simplified for the purposes of clarity of description, the output of only two of the flip-flops that constitute a part of password generator 64 are employed. In actual practice, as has been stated previously, more than two bits are

employed and more than one digit is displayed on display 18.

Before summarizing the operation of the circuit of Figure 4, initialization of the circuit will be described. Initialization occurs either at the time of manufacture or at some subsequent time when the key is to be introduced into commerce in combination with a specific computer software program to which access is to be limited. In the embodiment shown in Fgure 4, there are three inputs to which connection is necessary for initialization. Such inputs have been previously identified in connection with Figure 1 as contact points 22. One initialization input 22a, a data input, is coupled directly to the D input of flip-flop 100a. A second initialization input 22b, a clock input, is coupled to the clock inputs of flip-flops 106a—106d through a gating circuit. A third initialization input 22c, a load enable input, is directly coupled to one input of each of two AND gates 136 and 137 and is coupled through an inverter 138 to one input of each of two AND gates 107 and 110. The other input of AND gate 136 is coupled to the Q output of flip-flop 100d. The other input of AND gate 137 is coupled to clock input 22b. The outputs of AND gates 110 and 136 constitute the inputs to OR gate 112. During initialization only AND gates 136 and 137 are active because the load enable signal applied to initialization input 22c and inverted by inverter 138, disables AND gates 107 and 110.

In order to initialize the key, that is, to load into the shift register formed by flip-flops 100a—100d a permanent, unique number, an enable signal is first applied to load enable input 22c. The enable signal is a voltage level that corresponds to a logical 1. A serial bit pattern is then applied to data input 22a and a clock pulse signal, at a rate substantially in excess of that produced by divider circuit 60b, is applied to clock input 22c until flip-flops 100a—100d are loaded with the desired permanent bit pattern and flip-flops 106a—106d are loaded with an initial bit pattern. Thereafter connections to initialization inputs 22a, 22b and 22c are broken and the key is ready for use. Operation of key 12 will be described by using an example in which the bit pattern loaded into flip-flops 100a—100s is 0101, and the bit pattern initially loaded into flip-flops 106a—106d is 1100. Because flip-flops 116a—116d are reset prior to each introduction of a stimulus number, their respective Q outputs are set to a logical 0 state.

The output of password generator 64 is constituted by the outputs of flip-flops 116c and 116d which are coupled to display 18. The outputs of all flip-flops constituting password generator 64 are defined by the following equations:

$$Q_{116a}(t+1)=\text{stim}(t)\ \text{XOR}\ (Q_{116d}(t)\ \text{XOR}\ Q_{106d})$$
$$Q_{116b}(t+1)=Q_{116a}(t)\ \text{XOR}\ Q_{106a}(t)$$
$$Q_{116c}(t+1)=Q_{116b}(t)\ \text{XOR}\ Q_{106b}(t)$$
$$Q_{116d}(t+1)=Q_{116c}(t)\ \text{XOR}\ Q_{106c}(t)$$

In the above formulas Q(t) represents the state of the indicated parameter before a clock pulse is supplied by buffer register 124 to the flip-flops, the parameter Q(t+1) represents the state after such clock pulse, and the parameter stim represents the value of a bit in the stimulus number by sensors 28a—28d and processed by buffer register 124.

Referring to the table of Figure 5, rows 140 show a typical number permanently stored in the shift register constituted by flip-flops 100a—100d. Rows 142 show the number stored in the shift register constituted by flip-flops 106a—106d immediately after initialization, i.e., during day 0 in the operating life of the key. Rows 144 show that upon reset, the output of password generator 64, constituted by flip-flops 116a—116d, is constituted by all logical 0s. The next group 146 of four rows shows the outputs of flip-flops 116a—116d as each digit of a stimulus number 1110 is detected by sensors 28a—28d, processed by buffer register 124, and supplied to password generator 64 via circuit path 122. Upon completion of processing of the stimulus number, display 18 displays a number representative of binary 11 and indicated at 18_1.

Row group 148 shows the processing of a subsequent stimulus number, in this case 0100. The password displayed to the user by display 18 is representative of binary 10, indicated at 18_2.

When a timing pulse is produced by system clock 60a and divider 60b, the output states of flip-flops 106a—106d are changed, the new states being a function of the prior states of those flip-flops and the number permanently stored in flip-flops 100a—100d. Rows 150 show the state of flip-flops 106a—106d at day 1. If during day 1 the user wishes to use the device and if a stimulus number 1111 is produced by the computer system and received by sensors 28a—28d, indicated at row group 152, display 18 will display a number representative of binary 11, indicated at 18_3 in Figure 5.

The sequence of operation described above demonstrates that the password displayed to the user changes on a daily basis and changes for each stimulus number received from the computer system with which the device is used. Because the relation between the number permanently stored in flip-flops 100a—100d and the password characters displayed to the user is not an inverse relation, it is virtually impossible for even the legitimate possessor of the key to deduce the permanently stored number of the function or algorithm that is employed to generate the displayed password characters.

To afford further insight into the apparatus of Figures 3 and 4, the following pseudo code is presented to illustrate cooperation of a computer in which resides a program to which access is sought by a user and a key embodying the invention:

1) Prompt user for date;
2) Accept date from user;
3A) Compute internal baseword from date and stored seed;
3B) Generate stimulus number;

3C) Transmit stimulus number to user and save stimulus number;

3D) Compute internal password from internal baseword and saved stimulus number;

4) Prompt user for password;

5) Accept password from user;

6) Compare user password and internal password;

7) Initiate program execution if equal.

In the embodiment of the invention described in more detail in connection with Figure 2, the steps identified above as 3A—3D are combined and simplified to produce apparatus that affords security against unauthorized access to a somewhat lesser degree than the embodiment of the invention shown in Figures 3 and 4.

The elements in Figure 6 that are identical to similar elements in Figure 3 bear identical reference numerals to those employed in Figure 3. There is a pulse generator 60 which produces an output each day or like constant time interval. The timing pulse is coupled to baseword generator 62 where it is used as previously described. The baseword generated by baseword generator 62 is coupled to a password generator 64. Also coupled to password generator 64 is a stimulus number input from the video display via sensors 28a—28d, reception and processing of the stimulus number being indicated at 66. Password generator 64 produces a password that is displayed to the user on display 18 and the user inputs the password to the computer to obtain access to the protected software within the computer.

There are certain instances where the owner of software may desire to limit the usage made of the software. One form of limited usage is to permit the software user to access the software a specific number of times. To afford this mode of operation one enhancement in the device shown in Figure 6 is a usage counter 200. The usage counter is typically loaded at initialization time with a number equal to the authorized number of uses of the software. Each time a stimulus number is received and processed, as at 66, a pulse is applied to the usage counter via a signal path 202 to decrement the counter. When the counter is ultimately decremented to 0 the counter produces a disable signal on a signal path 204. The disable signal is coupled to password generator 64, and when the disable signal occurs, password generator 64 is disabled. Usage counter has an initialization input 22d so that at the time of initialization, the number of times for authorized usage can be loaded into the counter. Input 22d is accessible from a contact point 22 (Figure 1).

Another technique for limiting the usage of the software program is to place a time limit on the usage rather than a usage limit. For this purpose there is a time limit counter 206 which is loaded to some initial count indicating the number of days of authorized usage, there being an initialization input 22e for this purpose. A timing pulse from pulse generator 60 is supplied via a signal path 208 to time limit counter 206 each time a pulse is produced by pulse generator 60, e.g. one pulse per day. When the count stored in time limit counter reaches 0, a disable signal is produced on signal path 204 which disables password generator 64 and prevents further access to the program.

In the interest of completeness a power supply in the form of a battery 210 is shown in Figure 6. Such battery is also provided for the key shown in the other figures but it is not shown in the other figures in the interest of simplicity and clarity. Suffice it to say that the battery is connected to each of the elements within the circuit, the connections being indicated by an input lead having a plus sign, "+," adjacent the distal end thereof.

Thus it will be seen that the present invention provides a device that affords security against unauthorized access to computer software programs. Because the date represented by the cumulative number of pulses produced since initialization and the stimulus number are each modified according to one or more functions in producing a password visible to the user and because each function is not palpable, ascertainment of the password by reverse engineering or like analysis is so difficult as to be virtually impossible. The device is highly portable, convenient to use and relatively inexpensive to produce. In addition use of the device is convenient because no connection to or modification of the computer system is required.

Claims

1. A system for affording access by a user to a software program residing in a computer (34), comprising an access key (12) capable of generating a password and of being transported independently of the computer (34, 68) and an access key verification means adapted to be resident in the computer (34, 68) for verifying a password generated by the access key (12) and allowing access and use to the software program; characterised in that:

said access key (12) includes:

(a) pulse generating means (30, 60) for generating a signal that is dependent on the elapse of time;

(b) password generating means (32, 64) coupled to said pulse generating means (30, 60) for generating a password from the signal from said pulse generating means (30, 60);

(c) displaying means (18) communicating with the password generating means (32) for displaying at least part of said password; and

said access key verification means includes:

(a) means (40, 70) for receiving at least initially a time input;

(b) means (42, 72) for receiving the password as generated by the access key (12) and input by the user;

(c) means (46, 88) for processing the time input for producing an internal password;

(d) means (48, 49; 92, 94) for determining if the internal password bears a prescribed relationship

to the password generated by said access key (12);

(e) means (50, 96) for affording access to the software program if the prescribed relationship exists.

2. A system according to claim 1 wherein:

said pulse generating means (30, 60) includes means for generating in accordance with a prescribed algorithm a password comprised of a character string; and

said displaying means (18) includes means for displaying at least one character representative of said character string.

3. A system according to claim 1 or claim 2, wherein the computer has a video display (D), which can display another signal from the access key verification means, and wherein:

said access key verification means further includes:

(a) a stimulus number generating means (86) for generating a stimulus number;

(b) means for generating another signal on the video display (D) that is representative of said stimulus number; and

said access key further includes:

(a) at least one sensor (28) accessible from the exterior of said access key so that juxtaposition of the access key (12) and the display (D) affords excitation of the sensor (28) by the another signal;

(b) means (66) coupled to said sensor (28) for decoding the another signal to produce the stimulus number;

(c) said password generating means (62, 64) including a baseword generating means (62) communicating with said pulse generating means (60) for producing a baseword that is a function of the signal produced by said pulse generating means (60);

(d) said password generating means (62, 64) including a means (64) for combining the stimulus number with the baseword to produce the password.

4. A system according to claim 3 wherein said access key (12) includes:

means (200) for counting each time said sensor is excited by the another signal on the video display; and

means (206) for disabling said access key when the count on the counting means reaches a predetermined count.

5. A system according to claim 1 or claim 2, wherein the computer has a display, which can display another signal from the access key verification means, and wherein:

said access key verification means further includes:

(a) a stimulus number generating means for generating a stimulus number;

(b) means for generating another signal on the computer display that is representative of said stimulus number; and

said access key further includes:

(a) means for entering and decoding the another signal to produce the stimulus number;

(b) said password generating means including a baseword generating means communicating with said pulse generating means for producing a baseword that is a function of the signal produced by said pulse generating means;

(c) said password generating means including a means for combining the stimulus number with the baseword to produce the password.

6. A system according to claim 1 or claim 2, wherein said access key includes:

said signal from the pulse generating means providing a series of pulses;

a time limit counter means for counting pulses;

means for coupling said time limit counter means to said pulse generating means to count the number of pulses generated thereby; and

means for disabling said key when said time limit counter has counted a predetermined number of pulses from said pulse generating apparatus.

7. A system according to claim 1, or claim 2, wherein said password generating means of said access key comprises:

(a) a first register initialized to a fixed state that uniquely identifies the access key;

(b) a second register for selectively retaining the signal from the pulse generating means;

(c) means for coupling said pulse generating means to said second register;

(d) means for gating outputs of said first and second registers to produce said password; and said access key verification means includes:

(a) means for being initialized to a fixed state uniquely associated with the fixed state of said first register of said access key.

8. A system according to claim 7 with the computer having a video display which can display another signal from the access key verification means, wherein:

said access key verification means includes:

(a) means for generating a stimulus number;

(b) means for generating another signal on the video display that is representative of said stimulus number;

said access key includes:

(a) at least one sensor accessible from the exterior of said access key so that juxtaposition of the access key and the display affords excitation of the sensor by the another signal;

(b) a third register for selectively retaining the another signal on the video display;

(c) means for communicating the sensor to said third register so that the another signal can alter the state of the third register in accordance with the stimulus number; and

(d) said gating means includes means for gating an output from said third register with the output from said first and second registers to produce said password.

9. A system according to claim 7 wherein said access key includes:

a plurality of contacts means accessible from the exterior of said access key for initializing said access key;

means for coupling one of said contacts to said first register and another of said contacts to said second register; and

means for rendering the contacts immune to reinitialization.

10. A system according to claim 9 wherein said rendering means includes means for insulating said contacts after initialization.

11. A system according to claim 9, or claim 10, wherein said access key includes:

a third contact;

means for communicating said third contact with said gating means;

wherein said gating means includes means for enabling said first and second registers responsive to an initialization signal being applied to said third contact.

12. A system according to claim 1 or claim 2, wherein the computer has a video display which can display another signal from the access key verification means, wherein:

said access key verification means includes:

(a) a stimulus number generating means for generating a stimulus number;

(b) means for generating another signal on the video display that is representative of said stimulus number; and

said access key includes:

(a) at least one sensor accessible from the exterior of said access key so that juxtaposition of the access key and the display affords excitation of the sensor by the another signal;

(b) means coupled to said sensor for decoding the another signal to produce the stimulus number;

(c) said password generating means including a means for combining the stimulus number with the signal from the pulse generator to produce the password.

13. A system according to claim 1 or claim 2, wherein the computer has a display which can display another signal from the access key verification means, and wherein:

said access key verification means includes:

(a) a stimulus number generating means for generating a stimulus number;

(b) means for generating another signal on the computer display that is representative of said stimulus number; and

said access key includes:

(a) means for entering and decoding the another signal to produce the stimulus number;

(b) said password generating means including a means for combining the stimulus number with the signal from the pulse generator to produce the password.

14. A system according to claim 1, wherein

the password generating means of the access key is adapted to generate the password by encription of the signal from the pulse generating means, and

the means of the access key verification means for processing the time input is adapted to decrypt the password, so that the internal password is a decrypted password.

15. A system according to claim 14, wherein the computer has a video display which can display another signal from the access key verification means, and wherein:

said access key verification means includes:

(a) a stimulus number generating means for generating a stimulus number;

(b) means for generating another signal on the video display that is representative of said stimulus number; and

said access key includes:

(a) at least one sensor accessible from the exterior of said access key so that juxtaposition of the access key and the display affords excitation of the sensor by the another signal;

(b) means coupled to said sensor for decoding the another signal to produce the stimulus number;

(c) said password generating means including a means for encrypting the stimulus number with the signal from the pulse generating means to produce the password.

16. A system according to claim 15 including:

means for counting each time said sensor is excited by the video display of the computer;

means for disabling the access key when the counter reaches a predetermined count.

17. A system according to claim 14, wherein the computer has a display which can display another signal from the access key verification means, and wherein:

said access key verification means includes:

(a) a stimulus number generating means for generating a stimulus number;

(b) means for generating another signal on the computer display that is representative of said stimulus number; and

said access key includes:

(a) means for entering and decoding the another signal to produce the stimulus number;

(b) said password generating means including a means for encrypting the stimulus number with the signal from the pulse generating means to produce the password.

18. An access key (12) for affording access by a user to a software program, said access key comprising:

(a) pulse generating means (60) for generating a series of pulses that are dependent on the elapse of time;

(b) password generating means (62, 64) coupled to said pulse generating means for generating a password for one or more pulses from said pulse generating means (60);

(c) displaying means (18) communicating with the password generating means (62, 64) for displaying at least part of said password;

(d) at least one sensor (28) accessible from the exterior of said access key (12) so that a coded stimulus is receivable by said access key (12);

(e) means (60) coupled to said sensor for decoding the stimulus number;

(f) said password generating means for combining the stimulus number with the one or

more pulses from the pulse generator (60) to produce the password.

19. An access key according to claim 18 wherein said password generating means (62, 64) includes a baseword generating means (62) communicating with said pulse generating means (60) for producing a baseword that is a function of pulses produced by said pulse generating means (60); and

said password generating means (62, 64) further includes a means (64) for combining the stimulus number with the baseword to produce the password to afford a user access to a software program.

20. An access key according to claim 18, or claim 19 wherein said access key includes:

a time limit counter means for counting pulses;

means for coupling said time limit counter means to said pulse generating means to count the number of pulses generated thereby; and

means for disabling said access key when said time limit counter has counted a predetermined number of pulses from said pulse generating apparatus.

Patentansprüche

1. System zur Schaffung des Zugangs durch einen Benützer zu einem in einem Rechner (34) untergebrachten Softwareprogramm, umfassend einen Zugangsschlüssel (12), der fähig ist, ein Kennwort zu erstellen und unabhängig vom Rechner (34, 68) transportiert zu werden und eine Zugangsschlüssel-Nachprüfungseinrichtung, die dazu ausgebildet ist, im Rechner (34, 68) untergebracht zu werden, um ein Kennwort nachzuprüfen, das vom Zugansschlüssel (12) erstellt ist und den Zugang zum und die Verwendung des Softwareprogramms zuzulassen; dadurch gekennzeichnet daß

der genannte Zugangsschlüssel umfaßt:

(a) Impulsgebereinrichtungen (30, 60) zur Erzeugung eines Signals, das vom Zeitablauf abhängig ist;

(b) Kennworterstellungseinrichtungen (32, 64), die mit den genannten Impulsgebereinrichtungen (30, 60) gekoppelt sind, um ein Kennwort aus dem von den genannten Impulsgebereinrichtungen (30, 60) erzeugten Signal zu erstellen;

(c) eine Sichtanzeigeeinrichtung (18), die mit der Kennworterstellungseinrichtung (32) verbunden ist, um wenigstens einen Teil des genannten Kennwortes anzuzeigen; und

die genannte Zugangsschlüsselnachprüfungseinrichtung umfassend:

(a) Einrichtungen (40, 70) zum zumindest anfänglichen Empfang einer Zeiteingangsgröße;

(b) Einrichtungen (42, 72) zum Empfang des vom Zugangsschlüssel (12) erstellten und vom Benützer eingegebenen Kennwortes;

(c) Einrichtungen (46, 88) zur Verarbeitung der Zeiteingangsgröße, um ein internes Kennwort zu erstellen;

(d) Einrichtungen (48, 49; 92, 94) zur Bestimmung, ob das interne Kennwort in einem vorgeschriebenen Verhältnis zu dem von dem genannten Zugangsschlüssel (12) erstellten Kennwort steht;

(e) Einrichtungen (50, 96) zur Herstellung des Zugangs zum Softwareprogramm, wenn das vorgeschriebene Verhältnis besteht.

2. System nach Anspruch 1, worin

die genannten Impulsgebereinrichtungen (30, 60) Einrichtungen zur Erstellung eines Kennwortes aus einer Zeichenreihe gemäß einem vorgeschriebenen Algorithmus umfassen, welches Kennwort aus einer Zeichenreihe besteht; und

die genannte Sichtanzeigeeinrichtung (18) Mittel zur Sichtanzeige wenigstens eines für die genannte Zeichenreihe repräsentativen Zeichens aufweist.

3. System nach Anspruch 1 oder 2, worin der Rechner eine Videsichtanzeige (D) aufweist, die ein anderes Signal von der Zugangsschlüsselnachprüfungseinrichtung anzeigen kann, und worin

die genannte Zugangsschlüsselnachprüfungseinrichtung weiters umfaßt:

(a) eine Anregungsimpulszahlerzeugungseinrichtung (86) zur Erzeugung einer Anregungsimpulszahl;

(b) eine Einrichtung zur Erzeugung eines anderen Signals auf der Videosichtanzeige (D), das repreäsentativ für die genannte Anregungsimpulszahl ist; und

der genannte Zugangschlüssel weiters umfassend:

(a) wenigstens einen Sensor (28), der von außerhalb des genannten Zugangschlüssels zugänglich ist, sodaß eine Gegenüberstellung des Zugangsschlüssels, und der Sichtanzeige (D) die Erregung des Sensors (28) durch das andere Signal bewirkt;

(b) eine Einrichtung (66), die mit dem genannten Sensor (28) gekoppelt ist, um das andere Signal zu dekodieren und die Anregungsimpulszahl zu erzeugen;

(c) die genannte Kennworterstellungseinrichtung (62, 64) umfassend eine Basisworterstellungseinrichtung (62), die mit der genannten Impulsgebereinrichtung (60) in Verbindung steht, um ein Basiswort zu erstellen, das eine Funktion des Signals ist, das von der genannten Impulsgebereinrichtung (60) erzeugt wird;

(d) die genannte Kennworterstellungseinrichtung (62, 64) umfassend ein Mittel (64) zum Kombinieren der Anregungsimpulszahl mit dem Basiswort, um das Kennwort zu erstellen.

4. System nach Anspruch 3, worin der genannte Zugangsschlüssel (12) umfaßt:

eine Einrichtung (200) zum Zählen jedes Males, zu dem der Sensor durch das andere Signal auf der Videosichtanzeige erregt wird; und

eine Einrichtung (206) zum Sperren des genannten Zugangsschlüssels, wenn die Zählung auf der Zähleinrichtung einen vorgegebenen Wert erreicht.

5. System nach Anspruch 1 oder 2, worin der Rechner mit einer Sichtanzeige versehen ist, die fähig ist, ein anderes Signal der Zugangsschlüs-

selnachprüfungseinrichtung anzuzeigen, und worin

die genannte Zugangsschlüsselnachprüfungseinrichtung weiters umfaßt:

(a) eine Anregungsimpulszahlerzeugungseinrichtung zum Erzeugen einer Anregungsimpulszahl;

(b) eine Einrichtung zur Erzeugung eines anderen Signals auf der Rechnersichtanzeige, das repräsentativ für die genannte Anregungsimpulszahl ist; und

der genannte Zugangsschlüssel weiters umfassend:

(a) eine Einrichtung zum Eingeben und Dekodieren des anderen Signals, um die Anregungsimpulszahl zu erzeugen;

(b) die genannte Kennworterstellungseinrichtung umfassend eine Basisworterstellungseinrichtung, die mit der genannten Impulsgebereinrichtung in Verbindung steht, um ein Basiswort zu erstellen, das eine Funktion des Signals ist, das von der genannten Impulsgebereinrichtung erzeugt wird;

(c) die genannte Kennworterstellungseinrichtung weiters umfassend eine Einrichtung zum Kombinieren der genannten Anregungsimpulszahl mit dem Basiswort, um das Kennwort zu erstellen.

6. System nach Anspruch 1 oder 2, worin der genannte Zugangsschlüssel umfaßt:

das genannte Signal von der genannten Impulsgebereinrichtung, die eine Reihe von Impulsen erzeugt;

eine Zeitbegrenzungsezähleinrichtung zum Zählen von Impulsen;

eine Einrichtung zum Koppeln der genannten Zeitbegrenzungszähleinrichtung mit der genannten Impulsgebereinrichtung, um die von dieser erzeugte Anzahl von Impulsen zu zählen; und

eine Einrichtung zum Sperren des genannten Schlüssels, wenn der genannte Zeitbegrenzungszähler eine vorgegebene Anzahl von Impulsen von der genannten Impulsgebervorrichtung gezählt hat.

7. System nach Anspruch 1 oder 2, worin die genannte Kennworterstellungseinrichtung des genannten Zugangsschlüssels umfaßt:

(a) ein erstes Register, das zu einem fixierten bzw. festgesetzten Zustand initialisiert ist, der einzigartig den Zugangsschlüssel identifiziert;

(b) ein zweites Register zum selektiven Aufbewahren des Signals von der Impulsgebereinrichtung;

(c) eine Einrichtung zum Koppeln der genannten Impulsgebereinrichtung mit dem genannten zweiten Register;

(d) eine Einrichtung zum Torsteuern von Ausgängen des genannten ersten und zweiten Registers, um das genannte Kennwort zu erstellen; und die genannte Zugangsschlüsselnachprüfungseinrichtung umfassend:

(a) eine Einrichtung, die zu einem fixierten bzw. festgesetzten Zustand initialisiert wird, der auf einzigartige Weise mit dem festgesetzten Zustand des genannten ersten Registers des genannten Zugangsschlüssels assoziiert ist.

8. System nach Anspruch 7, in dem der Rechner mit einer Sichtanzeige versehen ist, die ein anderes Signal von der Zugangsschlüsselnachprüfungseinrichtung anzeigen kann, worin:

die genannte Zugangsschlüsselnachprüfungseinrichtung umfaßt:

(a) eine Einrichtung zum Erzeugen einer Anregungsimpulszahl;

(b) eine Einrichtung zum Erzeugen eines anderen Signals auf der Videosichtanzeige, das repräsentativ für die genannte Anregungsimpulszahl ist;

der genannte Zugangsschlüssel umfassend:

(a) wenigstens einen Sensor, der von außerhalb des genannten Zugangsschlüssels zugänglich ist, sodaß eine Gegenüberstellung des Zugangsschlüssels und der Sichtanzeige die Erregung des Sensors durch das andere Signal bewirkt;

(b) ein drittes Register für die selektive Aufbewahrung des anderen Signals auf der Videosichtanzeige;

(c) eine Einrichtung für die Verbindung des Sensors mit dem genannten dritten Register, sodaß das andere Signal den Zustand des dritten Registers in Übereinstimmung mit der Anregungsimpulszahl verändern kann; und

(d) die genannte Torsteuerungseinrichtung umfassend eine Einrichtung zum Torsteuern eines Ausgangs vom genannten dritten Register mit dem Ausgang des genannten ersten und zweiten Rewgister, um das genannte Kennwort zu erstellen.

9. System nach Anspruch 7, worin der genannte Zugangsschlüssel umfaßt:

eine Vielzahl von Kontakteinrichtungen, die von der Außenseite des genannten Zugangsschlüssels zugänglich sind, um den genannten Zugangsschlüssel zu initialiseren;

eine Einrichtung zum Koppeln eines der genannten Kontakte mit dem genannten ersten Register und eines anderen der genannten Kontakte mit dem genannten zweiten Register; und

eine Einrichtung, um die Kontakte immun gegen Reinitialisierung zu machen.

10. System nach Anspruch 9, worin die genannte Einrichtung zum Immunisieren der Kontakte eine Einrichtung zum Isolieren der genannten Kontakte nach der Initialisierung umfaßt.

11. System nach Anspruch 9 oder 10, worin der genannte Zugangsschlüsel umfaßt:

einen dritten Kontakt;

eine Einrichtung zum Verbinden des genannten dritten Kontaktes mit der genannten Torsteuerungseinrichtung;

worin die genannte Torsteuerungseinrichtung eine Einrichtung zur Freigabe des genannten ersten und zweiten Registers als Reaktion auf ein an den genannten dritten Kontakt angelegtes Initialisierungssignal umfaßt.

12. System nach Anspruch 1 oder 2, worin der Rechner eine Videosichtanzeige besitzt, die ein anderes Signal von der Zugangsschlüssel-nachprüfungseinrichtung anzeigen kann, worin:

die genannte Zugangsschlüsselnachprüfungseinrichtung umfaßt:

(a) eine Anregungsimpulszahlerzeugungseinrichtung für die Erzeugung einer Anregungsimpulszahl;

(b) eine Einrichtung zur Erzeugung eines anderen Signals auf der Videosichtanzeige, das repräsentativ für die genannte Anregungsimpulszahl ist; und

der genannte Zugangsschlüssel umfaßt:

(a) wenigstens einen Sensor, der von der Außenseite des genannten Zugangsschlüssels zugänglich ist, sodaß eine Gegenüberstellung des Zusangsschlüssels und der Videosichtanzeige die Erregung des Sensors durch das andere Signal bewirkt;

(b) eine Einrichtung, die mit dem genannten Sensor gekoppelt ist, um das andere Signal zu dekodieren und die Anregungsimpulszahl zu erzeugen;

(c) die genannte Kennworterstellungseinrichtung umfassend eine Einrichtung zum Kombinieren der Anregungsimpulszahl mit dem Signal des Impulsgebers, um das Kennwort zu erstellen.

13. System nach Anspruch 1 oder 2, worin der Rechner eine Sichtanzeige aufweist, die ein anderes Signal von der Zugangsschlüsselnachprüfungseinrichtung anzeigen kann und worin:

die genannte Zugangsschlüsselnachprüfungseinrichtung umfaßt:

(a) eine Anregungsimpulszahlerzeugungseinrichtung zum Erzeugen einer Anregungsimpulszahl;

(b) eine Einrichtung zum Erzeugen eines anderen Signals auf der Rechnersichtanzeige, das repräsentativ für die genannte Anregungsimpulszahl ist; und

der genannte Zugangsschlüssel umfaßt:

(a) eine Einrichtung zum Eingeben und Dekodieren des anderen Signals, um die Anregungsimpulszahl zu erzeugen;

(b) die genannte Kennworterstellungseinrichtung umfassend eine Einrichtung zum Kombinieren der Anregungsimpulszahl mit dem Signal von dem Impulsgeber, um das Kennwort zu erstellen.

14. System nach Anspruch 1, worin

die Kennworterstellungseinrichtung des Zugangsschlüssels dazu ausgebildet ist, das Kennwort durch Verschlüsseln des Signals von der Impulsgebereinrichtung zu erstellen und

die Einrichtung der Zugangsschlüsselnachprüfungseinrichtung zur Verarbeitung der Zeiteingabe dazu ausgebildet ist, das Kennwort zu entschlüsseln, sodaß das interne Kennwort ein entschlüsseltes Kennwort ist.

15. System nach Anspruch 14, worin der Rechner eine Videosichtanzeige aufweist, die ein anderes Signal von der Zugangsschlüsselnachprüfungseinrichtung anzeigen kann und worin:

die genannte Zugangsschlüsselnachprüfungseinrichtung umfaßt:

(a) eine Anregungsimpulszahlerzeugungseinrichtung zur Erzeugung einer Anregungsimpulszahl;

(b) eine Einrichtung zur Erzeugung eines anderen Signals auf der Videosichtanzeige, das repräsentativ für die genannte Anregungsimpulszahl ist; und

der genannte Zugangsschlüssel umfaßt:

(a) wenigstens einen Sensor, der von der Außenseite des genannten Zugangsschlüssels zugänglich ist, sodaß die Gegenüberstellung des Zugangsschlüssels und der Sichtanzeige die Erregung des Sensor durch das andere Signal bewirkt;

(b) eine Einrichtung, die mit dem genannten Sensor gekoppelt ist, um das andere Signal zu dekodieren und die Anrengungsimpulszahl zu erzeugen;

(c) die genannte Kennworterstellungseinrichtung umfassend eine Einrichtung zum Verschlüsseln der Anregungsimpulszahl mit dem Signal von der Impulsgebereinrichtung, um das Kennwort zu erstellen.

16. System nach Anspruch 15, umfassend:

eine Einrichtung zum Zählen jedes Males, zu dem der Sensor durch die Videosichtanzeige des Rechners erregt wird;

eine Einrichtung zum Sperren des Zugangsschlüssels, wenn der Zähler einen vorgegebenen Zählerstand bzw. eine vorgegebene Zählung erreicht.

17. System nach Anspruch 14, worin der Rechner eine Sichtanzeige besitzt, die ein anderes Signal von der Zugangsschlüsselnachprüfungseinrichtung anzeigen kann und worin:

die genannte Zugangsschlüsselnachprüfungseinrichtung umfaßt:

(a) eine Anregungsimpulszahlerzeugungseinrichtung zur Erzeugung einer Anregungsimpulszahl;

(b) eine Einrichtung zur Erzeugung eines anderen Signals auf der Rechnersichtanzeige, das repräsentativ für die genannte Anregungsimpulszahl ist; und

der genannte Zugangsschlüssel umfassend:

(a) eine Einrichtung zum Eingeben und Dekodieren des anderen Signals, um die Anregungsimpulszahl zu erzeugen;

(b) die genannte Kennworterstellungseinrichtung umfassend eine Einrichtung zum Verschlüsseln der Anregungsimpulszahl mit dem Signal der Impulsgebereinrichtung, um das Kennwort zu erstellen.

18. Zugangsschlüssel (12) zur Schaffung des Zugangs eines Benützers zu einem Softwareprogramm, der genannte Zugangsschlüssel umfassend:

(a) eine Impulsgebereinrichtung (60) zur Erzeugung eine Reihe von Impulsen, die vom Zeitablauf abhängig sind;

(b) Kennworteinrichtungen (62, 64), die mit der genannten Impulsgebereinrichtung gekoppelt sind, um ein Kennwort für einen oder mehrere Impulse der genannten Impulsgebereinrichtung (60) zu erstellen;

(c) eine Sichtanzeigeeinrichtung (18), die mit der Kennworterstellungseinrichtung (62, 64) in Verbindung steht, um wenigstens einen Teil des genannten Kennwortes anzuzeigen;

(d) wenigstens einen Sensor (28), der von der Außenseite des genannten Zugangsschlüssels (12) zugänglich ist, sodaß ein kodierter Anregungsimpuls vom genannten Zugangsschlüssel (12) empfangen werden kann;

(e) eine Einrichtung (60), die mit dem genannten Sensor zum Dekodieren der Anregungsimpulszahl gekoppelt ist;

(f) die genannte Kennworterstellungseinrichtung zum Kombinieren der Anregungsimpulszahl mit dem Impuls oder den Impulsen vom Impulsgeber (60), um das Kennwort zu erstellen.

19. Zugangsschlüssel nach Anspruch 18, worin die genannte Kennworterstellungseinrichtung (62, 64) eine Basisworterstellungseinrichtung (62) umfaßt, die mit der genannten Impulsgebereinrichtung (60) verbunden ist, um ein Basiswort zu erstellen, das eine Funktion von Impulsen it, die von der genannten Impulsgebereinrichtung (60) erzeugt werden; und

die genannten Kennworterstellungseinrichtungen (62, 64) weiters eine Einrichtung (64) zum Kombinieren der Anregungsimpulszahl mit dem Basiswort umfassen, um das Kennwort zu erstellen und einem Benützer Zugang zu einem Softwareprogramm zu verschaffen.

20. Zugangsschlüssel nach Anspruch 18 oder 19, worin der genannte Zugangsschlüssel umfaßt:

eine Zeitbegrenzungszähleinrichtung zum Zählen von Impulsen;

eine Einrichtung zum Koppeln der genannten Zeitbegrenzungszähleinrichtung mit der genannten Impulsgebereinrichtung, um die von dieser erzeugte Anzahl von Impulsen zu zählen; und

eine Einrichtung zum Sperren des genannten Zugangsschlüssels, wenn der genannte Zeitbegrenzungszähler eine vorgegebene Anzahl von Impulsen von der genannten Impulsgebereinrichtung gezählt hat.

Revendications

1. Un système pour permettre l'accès par un utilisateur à un programme de logiciel résidant dans un ordinateur (34), comprenant une clef d'accès (12) susceptible de produire un mot de passe et d'être transportée indépendamment de l'ordinateur (34, 68) et un moyen de vérification de la clef d'accès adapté pour être résidant dans l'ordinateur (34, 68) pour vérifier un mot de passe produit par la clef d'accès (12) et autorisant l'accès et l'utilisation au programme de logiciel; caractérisé en ce que:

ladite clef d'accès (12) comprend:

(a) un moyen de production d'impulsions (30, 60) pour produire un signal qui dépend de l'écoulement du temps;

(b) au moyen de production d'un mot de passe (32, 64) couplé au moyen de production d'impulsions (30, 60) pour produire un mot de passe à partir du signal du moyen de production d'impulsions (30, 60);

(c) un moyen de visualisation (18) comminiquant avec le moyen de production de mot de passe (32) pour visualiser au moins une partie dudit mot de passe; et

le moyen de vérification de la clef d'accès comprend:

(a) un moyen (40, 70) pour recevoir au moins initialement une entrée de temps;

(b) un moyen (42, 72) pour recevoir le mot de passe tel que produit par le clef d'accès (12) et entré par l'utilisateur;

(c) un moyen (46, 88) pour traiter l'entrée de temps pour produire un mot de passe interne;

(d) un moyen (48, 49; 92, 94) pour déterminer si le mot de passe interne porte une relation prescrite avec le mot de passe produit par ladite clef d'accès (12);

(e) un moyen (50, 96) pour permettre l'accès au programme de logiciel si la relation prescrite existe.

2. Un système selon la revendication 1 où:

le moyen de production d'impulsions précité (30, 60) comprend un moyen pour produire selon un algorithme prescrit un mot de passe constitué d'un train de caractères; et

le moyen de visualisation précité (18) comprend un moyen pour visualiser au moins un caractère représentatif dudit train de caractères.

3. Un système selon la revendication 1 ou la revendication 2, où l'ordinateur a un affichage vidéo (D), qui peut afficher un autre signal du moyen de vérification de la clef d'accès, et où:

le moyen de vérification de la clef d'accès comprend de plus:

(a) un moyen de production d'un nombre stimulant (86) pour produire un nombre stimulant;

(b) un moyen pour produire un autre signal sur l'affichage vidéo (D) qui est représentatif dudit nombre stimulant; et

la clef d'accès comprend de plus:

(a) au moins un détecteur (28) accessible de l'extérieur de ladite clef d'accès de sorte que la juxtaposition de la clef d'accès (12) et de l'affichage (D) permette l'excitation du détecteur (28) par l'autre signal;

(b) un moyen (66) couplé audit détecteur (28) pour décoder l'autre signal pour produire le nombre stimulant;

(c) le moyen de production du mot de passe (62, 64) comprenant un moyen de production d'un mot de base (62) communiquant avec le moyen de production d'impulsions (60) pour produire un mot de base qui est une fonction du signal produit par le moyen de production d'impulsions (60);

(d) le moyen de production du mot de passe (62, 64) comprenant un moyen (64) pour combiner le nombre stimulant au mot de base pour produire le mot de passe.

4. Un système selon la revendication 3 où la clef d'accès (12) précitée comprend:

un moyen (200) pour compter chaque fois que le détecteur précité est excité par l'autre signal sur l'affichage vidéo; et

un moyen (206) pour désactiver la clef d'accès lorsque le compte sur le moyen de comptage atteint un compte prédéterminé.

5. Un système selon la revendication 1 ou la revendication 2, où l'ordinateur a un affichage, qui peut afficher un autre du moyen de vérification de la clef d'accès et où:

le moyen de vérification de la clef d'accès comprend:

(a) un moyen de production d'un nombre stimulant pour produire un nombre stimulant;

(b) un moyen pour produire un autre signal à l'affichage de l'ordinateur qui est représentatif dudit nombre stimulant; et

la clef d'accès précitée comprend de plus:

(a) un moyen pour entrer et décoder l'autre signal pour produire le nombre stimulant;

(b) le moyen de production du mot de passe précité comprenant un moyen de production d'un mot de base communiquant avec le moyen de production d'impulsions pour produire un mot de base qui est une fonction du signal produit par le moyen de production d'impulsions;

(c) le moyen de production du mot de passe comprenant un moyen pour combiner le nombre stimulant au mot de base pour produire le mot de passe.

6. Un système selon la revendication 1 ou la revendication 2, où la clef d'accès comprend:

le signal précité du moyen de production d'impulsions produisant une série d'impulsions;

un moyen compteur de limitation de temps pour compter des impulsions;

un moyen pour coupler le moyen compteur de limite de temps au moyen de production d'impulsions pour compter le nombre d'impulsions produit ainsi; et

un moyen pour désactiver ladite clef lorsque le compteur de limite de temps a compté un nombre prédéterminé d'impulsions du dispositif d'impulsions.

7. Un système selon la revendication 1 ou la revendication 2, où le moyen de production du mot de passe précité de la clef d'accès précitée comprend:

(a) un premier registre initialisé à un état fixe qui identifie uniquement la clef d'accès;

(b) un second registre pour retenir sélectivement le signal du moyen de production d'impulsions;

(c) un moyen pour coupler le moyen de production d'impulsions audit second registre;

(d) un moyen pour synchroniser des sorties desdits premier et second registres pour produire ledit mot de passe; et le moyen de vérification de la clef d'accès comprend:

(a) un moyen pour être initialisé à un état fixe uniquement associé à l'état fixe dudit premier registre de ladite clef d'accès.

8. Un système selon la revendication 7 avec l'ordinateur ayant un affichage vidéo qui peut visualiser un autre signal du moyen de vérification de la clef d'accès, où:

le moyen de vérification de la clef d'accès comprend:

(a) un moyen pour produire un nombre stimulant;

(b) un moyen pour produire un autre signal sur l'affichage vidéo qui est représentatif dudit nombre stimulant;

la clef d'accès comprend:

(a) au moins un détecteur accessible de l'extérieur de ladite clef d'accès de sorte que la juxtaposition de la clef d'accès et de l'affichage permette l'excitation du détecteur par l'autre signal;

(b) un troisième registre pour retenir sélectivement l'autre signal à l'affichage vidéo;

(c) un moyen pour communiquer le détecteur dudit troisième registre de sorte que l'autre signal puisse modifier l'état du troisième registre selon la nombre stimulant; et

(c) le moyen de synchronisation comprend un moyen pour synchroniser une sortie du troisième registre à la sortie desdits premier et second registres pour produire ledit mot de passe.

9. Un système selon la revendication 7, où la clef d'accès comprend:

un certain nombre de moyens de contacts accessibles de l'extérieur de la clef d'accès pour initialiser la clef d'accès;

un moyen pour coupler l'un desdits contacts au premier registre précité et un autre desdits contacts au second registre précité; et

un moyen pour rendre le contact immunisé à la réinitialisation.

10. Un système selon la revendication 9, où le moyen rendant précité comprend un moyen pour isoler les contacts précités après initialisation.

11. Un système selon la revendication 9, ou la revendication 10, où la clef d'accès précitée comprend:

un troisième contact;

un moyen pour communiquer ledit troisième contact au moyen de synchronisation précité;

où le moyen de synchronisation comprend un moyen pour valider les premier et second registres précités en réponse à un signal d'initialisation appliqué au troisième contact.

12. Un système selon la revendication 1 ou la revendication 2, où l'ordinateur a un affichage vidéo qui peut visualiser un autre signal du moyen de vérification de la clef d'accès, où:

le moyen de vérification de la clef d'accès comprend:

(a) un moyen de production d'un nombre stimulant pour produire un nombre stimulant;

(b) un moyen pour produire un autre signal à l'affichage vidéo qui est représentatif dudit nombre stimulant; et

la clef d'accès comprend:

(a) au moins un détecteur accessible de l'extérieur de la clef d'accès de sorte que la juxtaposition de la clef d'accès et de l'affichage permette l'excitation du détecteur par l'autre signal;

(b) un moyen couplé audit détecteur pour décoder l'autre signal pour produire le nombre stimulant;

(c) le moyen de production du mot de passe comprenant un moyen pour combiner le nombre

stimulant au signal du générateur d'impulsions pour produire le mot de passe.

13. Un système selon la revendication 1 ou la revendication 2, où l'ordinateur a un affichage qui peut afficher un autre signal du moyen de vérification de la clef d'accès, et où:

le moyen de vérification de la clef d'accès comprend:

(a) un moyen de production d'un nombre stimulant pour produire un nombre stimulant;

(b) un moyen pour produire un autre signal à l'affichage de l'ordinateur qui est représentatif dudit nombre stimulant; et

la clef d'accès comprend:

(a) un moyen pour entrer et décoder l'autre signal pour produire le nombre stimulant;

(b) un moyen de production du mot de passe comprenant un moyen pour combiner le nombre stimulant au signal du générateur d'impulsions pour produire le mot de passe.

14. Un système selon la revendication 1 où

le moyen de production du mot de passe de la clef d'accès est adapté pour produire le mot de passe par encryptage du signal du moyen de production d'impulsions, et

le moyen du moyen de vérification de la clef d'accès pour traiter l'entrée de temps est adapté pour décrypter le mot de passe, de sorte que le mot de passe interne soit un mot de passe décrypté.

15. Un système selon la revendication 14, où l'ordinateur a un affichage vidéo qui peut visualiser un autre signal du moyen de vérification de la clef d'accès, et où:

le moyen de vérification de la clef d'accès comprend:

(a) un moyen de production d'un nombre stimulant pour produire un nombre stimulant;

(b) un moyen pour produire un autre signal à l'affichage vidéo qui est représentatif dudit nombre stimulant; et

la clef d'accès comprend:

(a) au moins un détecteur accessible de l'extérieur de la clef d'accès de sorte que la juxtaposition de la clef d'accès et de l'affichage permette l'excitation du détecteur par l'autre signal;

(b) un moyen couplé audit détecteur pour décoder l'autre signal pour produire le nombre stimulant;

(c) le moyen de production du mot de passe comprenant un moyen pour encrypter le nombre stimulant au signal de moyen de production d'impulsions pour produire le mot de passe.

16. Un système selon la revendication 15, comprenanant:

un moyen pour compter chaque fois que le détecteur est excité par l'affichage vidéo de l'ordinateur;

un moyen pour désactiver la clef d'accès lorsque le compteur atteint un compte prédéterminé.

17. Un système selon la revendication 14, où l'ordinateur a un affichage qui peut visualiser un autre signal du moyen de vérification de la clef d'accès, et où:

le moyen de vérification de la clef d'accès comprend:

(a) un moyen de production d'un nombre stimulant pour produire un nombre stimulant;

(b) un moyen pour produire un autre signal à l'affichage de l'ordinateur qui est représentatif dudit nombre stimulant; et

la clef d'accès comprend:

(a) un moyen pour entrer et décoder l'autre signal pour produire le nombre stimulant;

(b) un moyen de production du mot de passe comprenant un moyen pour encrypter le nombre stimulant avec le signal du moyen de production d'impulsions pour produire le mot de passe.

18. Une clef d'accès (12) pour permettre l'accès par un utilisateur à un programme de logiciel, la clef d'accès comprenant:

(a) un moyen de production d'impulsions (60) pour produire un série d'impulsions qui sont dépendantes de l'écoulement du temps;

(b) un moyen de production d'un mot de passe (62, 64) couplé au moyen de production d'impulsions pour produire un mot de passe pour l'une ou plusieurs impulsions du moyen de production d'impulsions (60);

(c) un moyen de visualisation (18) communiquant avec le moyen de production du mot de passe (62, 64) pour visualiser au moins une partie dudit mot de passe;

(d) au moins un détecteur (28) accessible de l'extérieur de la clef d'accès (12) de sorte qu'un nombre stimulant codé soit recevable par la clef d'accès (12);

(e) un moyen (60) couplé audit détecteur pour décoder le nombre stimulant;

(f) le moyen de production du mot de passe pour combiner le nombre stimulant à l'une ou plus des impulsions du générateur d'impulsions (60) pour produire le mot de passe.

19. Une clef d'accès selon la revendication 18 où le moyen de production du mot de passe (62, 64) comprend un moyen de production d'un mot de base (62) communiquant avec le moyen de production d'impulsions (60) pour produire un mot de base qui est une fonction des impulsions produites par le moyen de production d'impulsions (60); et

le moyen de production du mot de passe (62, 64) comprend de plus un moyen (64) pour combiner le nombre stimulant au mot de base pour produire le mot de passe pour permettre à un utilisateur d'accéder à un programme de logiciel;

20. Une clef d'accès selon la revendication 18, ou la revendication 19, où la clef d'accès comprend:

un moyen compteur de limite de temps pour compter des impulsions;

un moyen pour coupler ledit moyen compteur de limite de temps au moyen de production d'impulsions précité pour compter le nombre d'impulsions produites ainsi; et

un moyen pour désactiver la clef d'accès lorsque le compteur de limite de temps a compté un nombre prédéterminé d'impulsions du dispositif de production d'impulsions.